

On the Asymptotic Number of Generators of High Rank Arithmetic Lattices

Alexander Lubotzky, Raz Slutsky

Dedicated to Gopal Prasad on his 75th birthday

Abstract

Abert, Gelander and Nikolov [AGN17] conjectured that the number of generators $d(\Gamma)$ of a lattice Γ in a high rank simple Lie group H grows sub-linearly with $v = \mu(H/\Gamma)$, the co-volume of Γ in H . We prove this for non-uniform lattices in a very strong form, showing that for 2-generic such H 's, $d(\Gamma) = O_H(\log v / \log \log v)$, which is essentially optimal. While we can not prove a new upper bound for uniform lattices, we will show that for such lattices one can not expect to achieve a better bound than $d(\Gamma) = O(\log v)$.

1 Introduction

Let H be a connected, non-compact, simple real Lie group, with a fixed Haar measure μ . A discrete subgroup Γ of H is called a *lattice* if $\mu(H/\Gamma) < \infty$. It is called uniform (or co-compact) if H/Γ is compact, and non-uniform otherwise. In [Gel11], Gelander showed that there exists a constant $C_1 = C_1(H)$ such that $d(\Gamma) \leq C_1 \mu(H/\Gamma)$ where $d(\Gamma)$ is the minimal number of generators of such Γ . Recently, this was shown for other types of Lie groups [GS20].

In [AGN17, Conjecture 3], Abert, Gelander and Nikolov conjectured that if H is of high rank, *i.e.*, $\text{rank}_{\mathbb{R}}(H) \geq 2$, then $d(\Gamma)$ grows sub-linearly with $\mu(H/\Gamma)$.

The main goal of the present paper is to prove a strong form (essentially optimal) of this conjecture for the **non-uniform** lattices of H . We will make

some remarks on the uniform case, but at this stage, we are unable to prove the conjecture for this case. We do, however, give a lower bound on $d(\Gamma)$ for uniform lattices, demonstrating a distinction between the growth rates of the two classes.

Following [BL19], we say that H is 2-generic if the centre of the simply connected cover \tilde{H} of the split form of H is a 2-group, and \tilde{H} has no outer automorphisms of order three. This is the case for "most" H 's. In fact it holds for all H unless it is of type E_6, D_4 or A_n for $n \neq 2^m - 1$.

For convenience, and without loss of generality, we assume from now on that μ , the Haar measure on H , is normalized so that $\mu(H/\Gamma) > 1$ for every lattice Γ in H . This is possible since there is a lower bound on the co-volume of lattices due to Kazhdan and Margulis [KM68]. In addition, throughout this paper all logarithms are in base 2.

Our main result is the following.

Theorem 1.1. *Let H be a simple Lie group with $\mathbb{R}\text{-rank}(H) \geq 2$. Then there exists a constant $C_2 = C_2(H)$ such that*

(a) *For every non-uniform lattice Γ of H we have*

$$d(\Gamma) \leq C_2 \log(\mu(H/\Gamma))$$

(b) *If H is 2-generic, then for every non-uniform lattice Γ of H we have*

$$d(\Gamma) \leq C_2 \frac{\log(\mu(H/\Gamma))}{\log \log(\mu(H/\Gamma))}$$

We remark that we believe that the sharper bound of (b), which is best possible (see Section 4), holds for all H , but it depends (and actually equivalent to) some delicate number-theoretic conjectures. More precisely, Gauss' celebrated theorem [BS66, Theorem 8, p. 247] gives a very precise description of the order of the 2-torsion of the class group $Cl(k)$ of quadratic number fields k . From this theorem one deduces that $d_2(Cl(k)) = O(\frac{\log D_k}{\log \log D_k})$ where $d_2(Cl(k))$ is the number of generators of the 2-Sylow subgroup of $Cl(k)$ and D_k is the absolute value of the discriminant Δ_k of k . Now, if we would know

such bounds for the p -Sylow subgroups for the odd primes, then the estimate of (b) would follow for all H . In fact, this is essentially equivalent (See [BL19, Sections 3 and 7]).

However, despite much effort over the years, the current knowledge is quite far from having such bounds (see [PTBW20]).

The intimate connection between the group-theoretic/geometric statement of Theorem 1.1 and the delicate number theory is not as surprising as it seems at first sight. By the Margulis Arithmeticity Theorem [Mar91], every Γ in a high rank group H is an arithmetic lattice, and unlike the methods of [Gel11] and [AGN17], our method will use this fact extensively.

Our second result is based on the existence of infinite class field towers of totally real fields, due to Golod and Shafarevich [GS64], and follows the lines of [BL12]:

Theorem 1.2. *Let H be a simple Lie group of high rank. Then there exists a constant $C_3 = C_3(H)$ and a sequence of uniform lattices $\Gamma_i \leq H$ with $\mu(H/\Gamma_i) \rightarrow \infty$ such that*

$$d(\Gamma_i) \geq C_3 \log \mu(H/\Gamma_i)$$

This lower bound shows that the growth rate of $d(\Gamma)$ for uniform lattices is strictly larger than that of non-uniform ones, thus establishing a further distinction between the two types of lattices.

As in [BL12] and [BL19], the distinction stems from the fact that non-uniform lattices in H are defined over number fields of bounded degree over \mathbb{Q} , while the degrees of the number fields defining uniform lattices are unbounded.

Let us now describe the main line of the proof of Theorem 1.1.

Venkataramana [Ven87, Ven94] has developed a method to show that various subgroups of arithmetic groups are of finite index. This method uses unipotent elements and hence is valid only for non-uniform arithmetic lattices. This accumulates to the following result of Sharma and Venkataramana [SV05] which is a first main ingredient of our proof:

Theorem 1.3 [SV05, Theorem 1]. *Every high rank non-uniform arithmetic group Γ has a subgroup of finite index which is generated by at most three elements.*

It follows that if $\hat{\Gamma}$ is the pro-finite completion of Γ and $d(\hat{\Gamma})$ denotes the minimal number of topological generators of $\hat{\Gamma}$, then

$$d(\hat{\Gamma}) \leq d(\Gamma) \leq d(\hat{\Gamma}) + 3$$

Thus, it suffices to prove Theorem 1.1 for $d(\hat{\Gamma})$ rather than $d(\Gamma)$. Now, by a standard inverse limit argument, $d(\hat{\Gamma})$ is the supremum over $d(S)$ where S runs over finite quotients of Γ . Moreover, by a well-known result of Raghunathan [Rag76], non-uniform Γ 's satisfy the congruence subgroup property (denoted CSP from this point onwards), so we have to deal only with quotients by congruence subgroups. The proof for those will use some methods and techniques from [BL12, BL19] which in turn use crucially the seminal work of Prasad [Pra89]. These are valid in almost the same way for uniform and non-uniform lattices. Thus, the obstacle that prevents us from proving the conjecture in its full generality is the use of Theorem 1.3 and the fact that the CSP is known only for some uniform lattices.

For simplicity of the introduction, we treated in this introduction the case where H is simple, but similar results and methods apply to the case where H is semi-simple and Γ runs over all irreducible lattices, see Section 4.

This paper is dedicated to Gopal Prasad with admiration and affection. Prasad has made fundamental contributions to the arithmetic theory of algebraic groups. In particular, this paper is based on his seminal work on the co-volume of arithmetic lattices.

Acknowledgments. We would like to thank Andrei Rapinchuk and Igor Rapinchuk for helpful discussions and references.

The first author is indebted for support from the NSF (Grant No. DMS-1700165) and the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (Grant No. 692854). This material is based upon work supported by a grant from the Institute for Advanced Study.

The second author is indebted for support from the Israel Science Foundation grant ISF 2919/19, and would like to thank Tsachik Gelander for his continued support and guidance.

2 Principal Arithmetic Groups and Congruence Subgroups

Let H be a high rank simple connected linear Lie group, and let G be a semi-simple, simply connected, connected algebraic group defined over a number field k , with an epimorphism $\phi : G(k \otimes_{\mathbb{Q}} \mathbb{R}) \rightarrow H$ whose kernel is compact. Then $\phi(G(\mathcal{O}))$ and subgroups of H which are commensurable to it are called *arithmetic*. All irreducible lattices in higher rank arise as such [Mar91], and one of the key facts for our purposes is that for non-uniform lattices, the degree of k is bounded, where the bound depends only on H . Indeed, this follows from the well known result that H/Γ is non-compact if and only if Γ contains non-trivial unipotent elements (see [Mor15, Chapter 5.3]). Hence, $G(k \otimes_{\mathbb{Q}} \mathbb{R})$ has no compact factors, which implies that the number of Archimedean completions of k is bounded by the number of simple factors of H and so $[k : \mathbb{Q}]$ is bounded, and when H is simple, $[k : \mathbb{Q}] \leq 2$.

Let now Γ_0 be a maximal lattice in H . It is known (see [BP89, Prop. 1.4]) that in this setting, $\Gamma_0 = N(\Lambda')$ where Λ' is a nice arithmetic group, namely the *principal arithmetic subgroup* associated to a coherent family $(P_v)_{v \in V_f}$ of Parahoric subgroups in $G(k_v)$. More precisely,

$$\Lambda = \Lambda(P) = G(k) \cap \prod_{v \in V_f} P_v$$

where G is a k -form of H , V_f is the set of finite places of k , $P_v \subset G(k_v)$, and Λ' is the image of Λ in H , namely $\phi(\Lambda) = \Lambda' \subset H$.

Now, for every v there exists a smooth affine group scheme G_v defined over \mathcal{O}_v such that $G_v(\mathcal{O}_v) = P_v$ and $G_v(k_v)$ is k_v -isomorphic to $G(k_v)$. This induces a congruence subgroup structure on P_v defined as:

$$P_v(r) = \ker(G_v(\mathcal{O}_v) \rightarrow G_v(\mathcal{O}_v/\pi_v^r \mathcal{O}_v))$$

where π_v is a uniformizer of \mathcal{O}_v . These congruence subgroups induce a congruence structure on Λ , namely $\Lambda(\pi_v^r) = P_v(r) \cap \Lambda$. More generally, for every ideal I of \mathcal{O} look at its closure \bar{I} in $\hat{\mathcal{O}} = \prod_v \mathcal{O}_v$. Then \bar{I} is equal to $\prod_{i=1}^l \pi_{v_i}^{e_i} \hat{\mathcal{O}}$ for some $Y = \{v_1, \dots, v_l\} \subset V_f$ and $e_1, \dots, e_l \in \mathbb{N}$. We then define the I -

congruence subgroup of Λ ,

$$\Lambda(I) = \Lambda \cap \left(\prod_{i=1}^l P_{v_i}(e_i) \cdot \prod_{v \notin Y} P_v \right)$$

In particular, for every $m \in \mathbb{N}$, the m -congruence subgroup is defined as $\Lambda(m) := \Lambda(m\mathcal{O})$, and any subgroup of Λ which contains $\Lambda(I)$ for some $0 \neq I \triangleleft \mathcal{O}$ is called a congruence subgroup.

In the next few sections we use the congruence structure of such lattices to prove the main theorem. We will study Λ and Λ' interchangeably since an upper bound on $d(\Gamma)$ for Γ in Λ gives a similar bound on $d(\Gamma')$ for $\Gamma' = \phi(\Gamma)$ in Λ' .

2.1 Reduction to Subgroups of Principal Arithmetic Lattices

First, we use the fact that the index of these principal arithmetic subgroups $\Lambda' \leq \Gamma_0$ is bounded by a function of the co-volume of Γ_0 , and so we can work inside the principal arithmetic lattice while paying a negligible price. More precisely, we have by [BL19, Prop. 4.1]:

Proposition 2.1. *There exists a constant $C_4 = C_4(H)$ such that for every $Q = \Gamma_0/\Lambda'$ with $\mu(H/\Gamma_0) = v$ as above,*

$$(i) \quad |Q| \leq v^{C_4}$$

$$(ii) \quad \text{if } \Gamma_0 \text{ is non-uniform and } H \text{ is 2-generic, then } |Q| \leq C_4^{\log v / \log \log v}.$$

This enables us to reduce our main theorem to the following:

Theorem 2.2. *There exists a constant $C_5 = C_5(H)$ such that if Λ' is a non-uniform principal arithmetic group as above, and $\Gamma \leq \Lambda'$ a finite index subgroup of co-volume v , then $d(\Gamma) \leq C_5 \log(v)$. Furthermore, if H is 2-generic, we have $d(\Gamma) \leq C_5 \log(v) / \log \log(v)$.*

Let us first show how Theorem 2.2 and Proposition 2.1 imply the main Theorem 1.1.

Proposition 2.3. *Theorem 2.2 and Proposition 2.1 imply Theorem 1.1.*

Proof. Assume that H is 2-generic. Let Γ be a lattice in H of co-volume v and Γ_0 a maximal lattice containing it.

Let $\Gamma_0 = N(\Lambda')$ as above and $\Gamma' = \Gamma \cap \Lambda'$. By Proposition 2.1,

$$[\Gamma : \Gamma'] \leq C_4^{\log v / \log \log v} \leq v^{\log C_4}$$

Now, since $\mu(H/\Gamma) \leq v$ we have

$$\mu(H/\Gamma') \leq v^{1+\log C_4}$$

We can now use Theorem 2.2, to deduce:

$$\begin{aligned} d(\Gamma') &\leq C_5((\log v^{1+\log C_4}) / \log \log v^{1+\log C_4}) \\ &\leq C_5(1 + \log C_4) \frac{\log v}{\log \log v} = C_6 \frac{\log v}{\log \log v} \end{aligned}$$

Now, $\Gamma' = \Gamma \cap \Lambda' \trianglelefteq \Gamma$ and $\Gamma/\Gamma' \cong \Lambda'\Gamma/\Lambda'$. Using again Prop. 2.1 we deduce that

$$d(\Gamma/\Gamma') \leq (\log C_4) \frac{\log v}{\log \log v}$$

$$\text{Hence } d(\Gamma) \leq d(\Gamma') + d(\Gamma/\Gamma') \leq (C_6 + \log C_4) \frac{\log v}{\log \log v}.$$

The case when H is not 2-generic is similar and even slightly simpler. \square

3 Proof of the Upper Bound

3.1 Reduction to Congruence Subgroups

We wish to use the congruence subgroup property and Theorem 1.3 to further reduce the main theorem to a question about finite quotients of congruence subgroups. Notice that the arguments so far did not use the fact that the lattices are non-uniform. However, from now on, we are going to use Theorem 1.3, which is known only for non-uniform lattices, and the positive answer to the congruence subgroup problem for such lattices due to [Rag76].

First of all, we are going to pass to the pro-finite completion of Γ and Λ . This is due to the result of Sharma-Venkataramana in Theorem 1.3, which says that every non-uniform lattice has a finite index subgroup which is generated by at most 3 elements. It follows that for such lattices $d(\Gamma) \leq 3 + d(\widehat{\Gamma})$. In other words, it is enough to bound the number of generators of all finite quotients of Γ .

The second important assumption is the Congruence Subgroup Property.

Recall that $\Lambda = G(k) \cap \prod_{v \in V_f} P_v$. By the CSP, its pro-finite completion $\widehat{\Lambda}$ is essentially equal to its congruence completion. To be more precise, the congruence kernel, $C = \ker(\widehat{\Lambda} \rightarrow \prod_{v \in V_f} P_v)$ is finite, hence, $d(\widehat{\Lambda}) \leq d(C) + d(\overline{\Lambda})$ where $\overline{\Lambda}$ is the congruence completion of Λ .

Now, the result of [PR96] shows that the Margulis-Platonov conjecture and the CSP conjecture imply that C is cyclic. Thus, $d(\widehat{\Lambda}) \leq 1 + d(\overline{\Lambda})$. In the non-uniform case, both the Margulis-Platonov and the CSP conjecture are known, see [Rag76, PR10]. In addition, the same inequality holds for every finite index subgroup Γ of Λ . Hence altogether $d(\Gamma) \leq d(\widehat{\Gamma}) + 3 \leq d(\overline{\Gamma}) + 4$, where $\overline{\Gamma}$ is the congruence completion of Γ , which is in fact equal to the closure of Γ in $\prod_{v \in V_f} P_v$, by strong approximation [PR94, Thm 7.12].

Working now with the congruence completion and congruence subgroups, we use a quantitative version of the "level versus index" lemma, in order to pass to principal congruence subgroups.

Recall the classical lemma asserting that in $SL_2(\mathbb{Z})$, every congruence subgroup of index n contains $\Delta(m) = \ker(SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/m\mathbb{Z}))$ for some $m \leq n$. This lemma was later generalized in a quantitative manner in [BL12, Lemma 4.3, Remark 4.4]:

Lemma 3.1. *Let Λ be a principal arithmetic group in H with $\mu(H/\Lambda) \leq v$, then if Λ_1 is a congruence subgroup of Λ of index n , then $\Lambda(m\mathcal{O}) \subset \Lambda_1$ where $m \leq v^{C_7}n$, C_7 depends only on H , and $\Lambda(m\mathcal{O})$ is the principal congruence subgroup of level m .*

In addition, if we restrict to non-uniform lattices, we have that

$$[\Lambda : \Lambda(m\mathcal{O})] \leq (vn)^{C_8}$$

Let now $\Gamma \leq \Lambda$ be a congruence subgroup with $\mu(G/\Gamma) \leq v$. By our assumption on μ we have that $\mu(G/\Lambda) \geq 1$, thus the index of Γ in Λ is also bounded by v , and using 3.1 we have

$$d(\Gamma) \leq d(\Lambda(m\mathcal{O})) + d(\Gamma/\Lambda(m\mathcal{O}))$$

where $m \leq v^{C_7+1}$. We shall now analyse the number of generators of these two factors.

3.2 Rank of Principal Congruence Subgroups and of Finite Congruence Quotients

So far, we have reduced the problem to bounding:

- (i) $d(\Lambda(m\mathcal{O}))$, and
- (ii) $d(\Gamma/\Lambda(m\mathcal{O}))$

In order to do so we will need the following definition and proposition:

Definition 3.2. *Let G be a pro-finite group, then the Prüfer rank or subgroup rank of G is defined as:*

$$\text{rank}(G) := \sup\{d(H) \mid H \leq G\}$$

where H runs over the closed subgroups of G and $d(H)$ denotes the minimal number of topological generators of H .

It is easy to see that if $H \leq G$ and K is a quotient of H then $\text{rank}(K) \leq \text{rank}(G)$. Also, if $1 \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow 1$ is an exact sequence of pro-finite groups then $\text{rank}(G_2) \leq \text{rank}(G_1) + \text{rank}(G_3)$.

The following proposition will be used several times later on:

Proposition 3.3. *Let $d, s \in \mathbb{N}$, then $\exists C_9 = c(d, s) \leq 3d^2s^2$ such that if k/\mathbb{Q} is a number field of degree d and \mathcal{O} its ring of integers, then*

(a) For every finite place $v \in V_f$ of k ,

$$\text{rank}(SL_s(\mathcal{O}_v)) \leq C_9$$

(b) For every rational prime p ,

$$\text{rank}\left(\prod_{v|p} SL_s(\mathcal{O}_v)\right) \leq d \cdot C_9$$

Proof. Denote the first congruence subgroup by $\Gamma_v(1) := \ker(SL_s(\mathcal{O}_v) \rightarrow SL_s(\mathbb{F}_{q_v}))$ where \mathbb{F}_{q_v} is the residue field of \mathcal{O}_v . Since \mathcal{O}_v is the integral closure of \mathbb{Z}_p in k_v , we can embed $SL_s(\mathcal{O}_v)$ in $SL_{sd}(\mathbb{Z}_p)$. The congruence subgroup $\Gamma_v(1)$ is thus a subgroup of $\ker(SL_{sd}(\mathbb{Z}_p) \rightarrow SL_{sd}(\mathbb{F}_p))$ which is powerful pro- p of rank $\leq s^2 d^2$ [DdSMS99, Theorem 5.2, and Theorem 3.8], thus $d(\Gamma_v(1)) \leq s^2 d^2$. Now, since $\text{rank}(SL_s(\mathcal{O}_v)) \leq \text{rank}(\Gamma_v(1)) + \text{rank}(SL_s(\mathcal{O}_v)/\Gamma_v(1))$, it remains to bound the rank of the finite quotient $SL_s(\mathcal{O}_v)/\Gamma_v(1)$. By the same argument above, this is a subgroup of $SL_{sd}(\mathbb{F}_p)$. By [LS03, Cor. 24, p. 326], $\text{rank}(GL_{sd}(\mathbb{F}_p)) \leq 2s^2 d^2$, and so we get the bound in (a) with $c(d, s) = 3d^2 s^2$. The second part follows immediately as the number of finite places above p is at most d , the degree of the field extension. \square

Let us note that the proposition immediately implies the bound needed in (ii), i.e., a bound on $d(\Gamma/\Lambda(m\mathcal{O}))$. Indeed, $\Gamma/\Lambda(m\mathcal{O}) = \overline{\Gamma}/\overline{\Lambda}(m\mathcal{O})$ is a quotient of an open subgroup of $\prod_{p|m} \prod_{v|p} P_v$. By the prime number theorem, the number of primes dividing m is bounded by $\frac{\log m}{\log \log m}$, and as $P_v \subset SL_s(\mathcal{O}_v)$ where s is some fixed number such that $H \subset SL_s(-)$, Proposition 3.3 implies that $\text{rank}(\prod_{v|p} P_v) \leq dC_9$. Altogether, we have that $d(\Gamma/\Lambda(m\mathcal{O})) \leq C_{10} \frac{\log m}{\log \log m}$, as needed.

In order to bound $d(\Lambda(m\mathcal{O}))$ we need a more delicate argument. Let us formulate it as a Lemma:

Lemma 3.4. *Let H be a simple Lie group of higher rank, and $\Lambda(m\mathcal{O})$ a principal congruence subgroup of a non-uniform principal arithmetic group Λ in H as above, then there exists a constant $C_{10} = C_{10}(H)$ such that*

$$d(\Lambda(m\mathcal{O})) \leq C_{10} \frac{\log m}{\log \log m}$$

Proof. Following the discussion in Section 3.1, $d(\Lambda(m\mathcal{O})) \leq d(\overline{\Lambda(m\mathcal{O})}) + 4$ where $\overline{\Lambda(m\mathcal{O})}$ is the congruence completion of $\Lambda(m\mathcal{O})$. If $m = \prod_{i=1}^l p_i^{e_i}$, then by the strong approximation theorem, $\overline{\Lambda(m\mathcal{O})} = A \times B \times C$ where:

- $A = \prod_{i=1}^l A_{p_i}$, where each A_{p_i} is a product of pro- p_i groups, one for each v dividing p_i .
- $B = \prod_{v \in T} P_v$ where $T = \{P_v \text{ is not hyper-special, and } v \nmid m\}$
- $C = \prod_{v \in T'} P_v$ where $T' = \{P_v \text{ is hyper-special, and } v \nmid m\}$.

We have to bound each of $d(A)$, $d(B)$, and $d(C)$.

For A : this is a product of (finitely many) pro- p groups, for different p 's, each of rank at most dC_9 by Proposition 3.3, so its rank, being a pro-nilpotent group, is also bounded by dC_9 . For bounding B , we recall [BL12, Prop. 4.1] and the discussion in [Bel07, Section 6.2], which implies that $|T| = O_H(\log m / \log \log m)$. Using again Proposition 3.3, we deduce that $d(B) \leq \text{rank}(B) \leq C_{11} \log m / \log \log m$. Finally, let us deal with C . First, a warning: C is a product of infinitely many P_v 's and its rank is not bounded. Still, $d(C)$ is bounded. To see this, let us recall the local structure of hyper-special Parahoric subgroups.

Let G be an absolutely almost-simple simply connected algebraic group over a non-archimedean local field K_v , and let $P_v \subset G(K_v)$ be a hyper-special parahoric subgroup. Then $P_v = \mathcal{G}(\mathcal{O}_v)$, where \mathcal{G} is a reductive group scheme over the valuation ring $\mathcal{O}_v \subset K_v$ with generic fiber G (cf. [Tit79, 3.8]). It is known (cf. [SGA70, Exp. XXII, Proposition 2.8]) that the reduction $\underline{\mathcal{G}}$ is also an absolutely almost-simple simply connected algebraic group over the residue field k_v , which is in fact quasi-split by Lang's theorem. The group $\underline{\mathcal{G}}(k_v)$ is then quasi-simple group provided $|k_v| \geq 5$ (cf. [Ste16, §4, 11], [Tit64]). On the other hand, there is the reduction map $\mathcal{G}(\mathcal{O}_v) \rightarrow \underline{\mathcal{G}}(k_v)$, the kernel of which (the congruence subgroup modulo the valuation ideal $\mathfrak{p}_v \subset \mathcal{O}_v$) is a pro- p group for $p = \text{char } k_v$. Thus, P_v has a normal subgroup which is a pro- p group, with the quotient being a quasi-simple group.

In our situation, this means that if P_v is hyper-special, then P_v is an extension of $P_v(1)$, a pro- p group of bounded rank (actually bounded by $d^2 s^2$), by a quasi-simple group of the form $G_v(\mathbb{F}_{q_v})$ where \mathbb{F}_{q_v} is the residue field of v . Now, $\prod_{v \in T'} P_v(1)$ is a product of infinitely many pro- p groups (at

most d for every p) each of rank at most $s^2 d^2$, so $\text{rank}(\prod_{v \in T'} P_v(1)) \leq s^2 d^3$. At the same time $C / \prod_{v \in T'} P_v(1) = \prod_{v \in T'} G_v(\mathbb{F}_{q_v})$ is a product of infinitely many quasi-simple finite groups, in which the multiplicity of every simple quotient is bounded by at most d . An elementary argument, keeping in mind that every finite quasi-simple group is generated by two elements, implies that the product is generated by at most $2d$ elements and thus $d(C) \leq d^3 s^2 + 2d$. \square

Recall that in Section 3.1 we had $m \leq v^{C_7+1}$, so the proof of Theorem 2.2, and hence also the proof of our main result, Theorem 1.1, is now complete. \square

The proof of Lemma 3.4 yields the following interesting observation: The bounds on $d(A)$ and $d(C)$ there were absolute (depending on H , but not on m). Thus, if $T = \emptyset$, i.e., if for all $v \in V_f$ P_v is hyper-special, as it is for example if we take a Chevalley group scheme, there is an absolute bound on the number of generators of principal congruence subgroups. One can even work out the bounds to deduce:

Corollary 3.5. *Let G be a Chevalley group scheme and \mathcal{O} the ring of integers in a number field k with $[k : \mathbb{Q}] = d$. Then for every $I \not\subseteq \mathcal{O}$,*

$$d(G_{\mathcal{O}}(I)) \leq d \cdot \dim(G) + 4$$

where $G_{\mathcal{O}}(I) = \ker(G(\mathcal{O}) \rightarrow G(\mathcal{O}/I))$.

This is a pretty sharp estimate, as one can see that $d(G_{\mathcal{O}}(I)) \geq d \cdot \dim(G)$.

Let us just stress that the absolute bound is valid only for the principal congruence subgroups, but not for all congruence subgroups. In fact, a residually finite group with an absolute bound on the number of generators of its finite index subgroups must be virtually solvable ([LM89]). See Section 4 for more.

4 Between Uniform and Non-Uniform Lattices

The bound $d(\Gamma) = O_H(\frac{\log v}{\log \log v})$ with $v = \mu(H/\Gamma)$ which was proved in Theorem 1.1 for non-uniform lattices Γ in 2-generic simple Lie groups H is best

possible. In fact, even if we take any lattice Λ in H and look only on its finite index subgroups we can not do better. Moreover, this is true for every non virtually solvable group. More precisely:

Proposition 4.1. *Let $n \in \mathbb{N}$, F a field of characteristic $p \geq 0$, and Γ a finitely generated infinite subgroup of $GL_n(F)$ which is not virtually solvable. Then there exists a constant $c > 0$ and finite index subgroups Γ_i of Γ with $n_i := [\Gamma : \Gamma_i] \rightarrow \infty$, such that*

(a) *If $p = 0$,*

$$d(\Gamma_i) \geq c \frac{\log n_i}{\log \log n_i}$$

(b) *If $p > 0$,*

$$d(\Gamma_i) \geq c \log n_i$$

Proof. As Γ is finitely generated and not virtually solvable, it has a specialization $\varphi : \Gamma \rightarrow GL_n(k)$ for some global field k of characteristic p , where $\varphi(\Gamma)$ is also not virtually solvable ([LL04, Thm 4.1]). As proving the result for $\varphi(\Gamma)$ implies it for Γ , we can assume that $\Gamma \subset GL_n(k)$. Furthermore, if G is the Zariski closure of Γ , it is not virtually solvable, and so we can divide by its radical in order to assure that G is semi-simple. We are also allowed to replace Γ by a group commensurable to it. Hence we can assume altogether that G is simple, connected and even simply connected, defined over k . As Γ is finitely generated, it is inside the \mathcal{O}_S -points of G , i.e., Γ is a Zariski dense subgroup of an S -arithmetic subgroup Λ of G .

Assume now that $p = \text{char}(F) = 0$. By the Strong Approximation Theorem for linear groups [LS03, P. 391], Γ is dense in the S -arithmetic group Λ with respect to the congruence topology of Λ . More precisely, it implies that $\widehat{\Gamma}$ is mapped onto $\overline{\Lambda_0}$, where Λ_0 is a finite index subgroup of Λ , and $\overline{\Lambda_0}$ is its congruence completion. So, it suffices to prove the result for $\overline{\Lambda_0}$. From now on, $d(H)$ denotes the minimal number of topological generators of a group H . Again, we can replace Λ_0 by a principal arithmetic group Λ , defined similarly to the one defined in Section 2, and so $\Lambda = G(k) \cap \prod_{v \in V_f \setminus S} P_v$ where this time v runs over the finite valuations which are not in the finite set S , and $\overline{\Lambda} = \prod_{v \in V_f \setminus S} P_v$ by the Strong Approximation Theorem.

Let x be a large real number, $P(x)$ the set of rational primes less than x and m their product. By the prime number theorem $|P(x)| \sim \frac{x}{\log x}$ and $m \sim e^x$. For all large enough $p \in P(x)$, $\overline{\Lambda}/\overline{\Lambda(p)}$ is a product of finite quasi-simple

groups and hence its order is divisible by 2. As $\overline{\Lambda}/\overline{\Lambda(m)} = \prod_{p \in P_x} \overline{\Lambda}/\overline{\Lambda(p)}$, the group $\overline{\Lambda}/\overline{\Lambda(m)}$ contains a subgroup isomorphic to \mathbb{F}_2^l with $l \sim |P(x)|$. Let Γ' be the pre-image of this subgroup in $\overline{\Lambda}$. Then $[\overline{\Lambda} : \Gamma'] \leq |\overline{\Lambda}/\overline{\Lambda(m)}| \leq m^{C'}$ for some constant C' , while $d(\Gamma') \geq l \sim \frac{x}{\log x} \sim \frac{\log m}{\log \log m}$ and the proposition is proved for the first case. The reader may recognize the last argument is a quantitative use of the general "Lubotzky Alternative", see [LS03, P. 400].

We turn now to the positive characteristic case. Here our lower bound is stronger, and despite that, the proof is easier. The lower bound follows already from any local completion: As Γ is Zariski dense in G , the closure of Γ is open in the v -adic topology of $G(k_v)$, namely, it is commensurable with $G(\mathcal{O}_v)$. Now, $\mathcal{O}_v \cong \mathbb{F}_q[[t]]$ for some $q = p^e$ (where e depends on the choice of v). If we denote $K = G(\mathcal{O}_v) = G(\mathbb{F}_q[[t]])$, and look at the congruence subgroup $K(i) = \ker(G(\mathbb{F}_q[[t]]) \rightarrow G(\mathbb{F}_q[t]/(ti)))$, then $K(i)$ is a subgroup of K of index approximately $q^{i \dim G}$. At the same time, $[K(i), K(i)] \subset K(2i)$, and $K(i)^p \subset K(pi) \subset K(2i)$. Hence $d(K(i))$ is at least ie_v . (see [LS94] for more detailed arguments of this fact, and in particular Prop. 4.3 there which shows that this estimate is sharp). This proves (b). \square

The proposition shows that, in particular, in every lattice Λ in a non-compact simple Lie group H , there exists a sequence Λ_i of co-volumes v_i going to infinity with $d(\Lambda_i) \geq c \frac{\log v_i}{\log \log v_i}$. Theorem 1.1 shows that this is sharp even if we consider all the non-uniform lattices in H (at least when H is 2-generic). On the other hand, Theorem 1.2 tells us that this bound can never be true if we take all the uniform lattices together. Let us recall its formulation again here:

Theorem 4.2. *Let H be a connected simple Lie group of rank ≥ 1 . Then there exist $c > 0$ and a sequence Γ_i of uniform lattices in H such that $\mu(H/\Gamma_i) \rightarrow \infty$ and $d(\Gamma_i) \geq c \log(\mu(H/\Gamma_i))$*

This theorem is essentially proved in [BL12, Thm 1(i)] for a different goal. Let us therefore only sketch the proof.

Proof. It is shown there, based on the Golod-Shafarevich [GS64] construction of infinite class field towers that there exists an infinite sequence of field extensions k_i of \mathbb{Q} of degree $d_i = d_{k_i} \rightarrow \infty$ and $rd_i := \mathcal{D}_{k_i}^{1/d_i}$ bounded, where \mathcal{D}_{k_i} is the absolute value of the discriminant of k_i . Moreover, using a result

of Prasad and Rapinchuk [PR06], these k_i can be chosen in such a way that they give rise to principal arithmetic lattices Λ_i of H of co-volume at most $c_1^{d_i}$ (for a constant $c_1 > 0$ depending only on H), and such that for some fixed rational prime p , $\Lambda_i/\Lambda_i(p)$ is a quasi-semi-simple finite group of the form $G_i(p^{e_i})$ of order at most $p^{d_i \dim(H)}$. This finite group contains a (root) subgroup isomorphic to $\mathbb{F}_{p^{d_i}} \cong (\mathbb{F}_p)^{d_i}$ and the pre-image of it, Γ_i , satisfies therefore $d(\Gamma_i) \geq d_i$ while $\mu(H/\Gamma_i) \leq p^{d_i \dim H} \cdot c_1^{d_i} = (c_1 p^{\dim H})^{d_i}$, which proves the Theorem. \square

We end the paper by a remark on semi-simple groups H . Essentially, the proof of Theorem 1.1 works for irreducible non-uniform lattices in such H , except that for a general semi-simple group, the degree of the field of definition of non-uniform lattices can be larger than 2, although still bounded. Thus, Gauss' Theorem which was used in Proposition 2.1 is not known. Therefore, for such (high rank) H , we can prove only the weaker statement, namely: for every irreducible non-uniform lattice Γ , $d(\Gamma) \leq O_H(\log \mu(H/\Gamma))$, while we still believe that the right bound is $O_H(\log(\mu(H/\Gamma))/\log \log(\mu(H/\Gamma)))$. The reader is referred to [BL19, Section 7] for a discussion of the connection between such group theoretic/geometric conjectures and number theoretic open problems.

References

- [AGN17] Miklos Abert, Tsachik Gelander, and Nikolay Nikolov. Rank, combinatorial cost, and homology torsion growth in higher rank lattices. *Duke Math. J.*, 166(15):2925–2964, 2017.
- [Bel07] Mikhail Belolipetsky. Counting maximal arithmetic subgroups. *Duke Math. J.*, 140(1):1–33, 2007. With an appendix by Jordan Ellenberg and Akshay Venkatesh.
- [BL12] Mikhail Belolipetsky and Alexander Lubotzky. Manifolds counting and class field towers. *Adv. Math.*, 229(6):3123–3146, 2012.
- [BL19] Mikhail Belolipetsky and Alexander Lubotzky. Counting non-uniform lattices. *Israel J. Math.*, 232(1):201–229, 2019.

- [BP89] Armand Borel and Gopal Prasad. Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups. *Inst. Hautes Études Sci. Publ. Math.*, 69(1):119–171, 1989.
- [BS66] A. I. Borevich and I. R. Shafarevich. *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966.
- [DdSMS99] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro- p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.
- [Gel11] Tsachik Gelander. Volume versus rank of lattices. *J. Reine Angew. Math.*, 661:237–248, 2011.
- [GS64] E. S. Golod and I. R. Safarevič. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.
- [GS20] Tsachik Gelander and Raz Slutsky. On the minimal size of a generating set of lattices in Lie groups. *J. Lie Theory*, 30(1):33–40, 2020.
- [KM68] D. A. Každan and G. A. Margulis. A proof of Selberg’s hypothesis. *Mat. Sb. (N.S.)*, 75 (117):163–168, 1968.
- [LL04] Michael Larsen and Alexander Lubotzky. Normal subgroup growth of linear groups: the (G_2, F_4, E_8) -theorem. In *Algebraic groups and arithmetic*, pages 441–468. Tata Inst. Fund. Res., Mumbai, 2004.
- [LM89] Alexander Lubotzky and Avinoam Mann. Residually finite groups of finite rank. *Math. Proc. Cambridge Philos. Soc.*, 106(3):385–388, 1989.
- [LS94] Alexander Lubotzky and Aner Shalev. On some Λ -analytic pro- p groups. *Israel J. Math.*, 85(1-3):307–337, 1994.
- [LS03] Alexander Lubotzky and Dan Segal. *Subgroup growth*, volume 212 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2003.

- [Mar91] G. A. Margulis. *Discrete subgroups of semisimple Lie groups*, volume 17 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1991.
- [Mor15] Dave Witte Morris. *Introduction to arithmetic groups*. Deductive Press, 2015.
- [PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.
- [PR96] Gopal Prasad and Andrei S. Rapinchuk. Computation of the metaplectic kernel. *Inst. Hautes Études Sci. Publ. Math.*, 84(1):91–187, 1996.
- [PR06] Gopal Prasad and Andrei S. Rapinchuk. On the existence of isotropic forms of semi-simple algebraic groups over number fields with prescribed local behavior. *Adv. Math.*, 207(2):646–660, 2006.
- [PR10] Gopal Prasad and Andrei S Rapinchuk. Developments on the congruence subgroup problem after the work of bass, milnor and serre. *Collected papers of John Milnor. V: Algebra (ed. H. Bass and TY Lam)*, Amer. Math. Soc., Providence, RI, 2010.
- [Pra89] Gopal Prasad. Volumes of S -arithmetic quotients of semi-simple groups. *Inst. Hautes Études Sci. Publ. Math.*, 69(1):91–117, 1989. With an appendix by Moshe Jarden and the author.
- [PTBW20] Lillian B. Pierce, Caroline L. Turnage-Butterbaugh, and Melanie Matchett Wood. An effective Chebotarev density theorem for families of number fields, with an application to ℓ -torsion in class groups. *Invent. Math.*, 219(2):701–778, 2020.
- [Rag76] M. S. Raghunathan. On the congruence subgroup problem. *Inst. Hautes Études Sci. Publ. Math.*, 46(1):107–161, 1976.
- [SGA70] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*. Séminaire de Géométrie

Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 152. Springer-Verlag, Berlin-New York, 1970.

- [Ste16] Robert Steinberg. *Lectures on Chevalley groups*, volume 66 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2016.
- [SV05] R. Sharma and T. N. Venkataramana. Generations for arithmetic groups. *Geom. Dedicata*, 114:103–146, 2005.
- [Tit64] J. Tits. Algebraic and abstract simple groups. *Ann. of Math. (2)*, 80:313–329, 1964.
- [Tit79] J. Tits. Reductive groups over local fields. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, pages 29–69. Amer. Math. Soc., Providence, R.I., 1979.
- [Ven87] T. N. Venkataramana. Zariski dense subgroups of arithmetic groups. *J. Algebra*, 108(2):325–339, 1987.
- [Ven94] T. N. Venkataramana. On systems of generators of arithmetic subgroups of higher rank groups. *Pacific J. Math.*, 166(1):193–212, 1994.

Alexander Lubotzky, INSTITUTE OF MATHEMATICS, HEBREW UNIVERSITY, JERUSALEM 91904, ISRAEL.

E-mail address: `alex.lubotzky@mail.huji.ac.il`

Raz Slutsky, DEPARTMENT OF MATHEMATICS. WEIZMANN INSTITUTE OF SCIENCE. REHOVOT 76100, ISRAEL.

E-mail address: `razslo@gmail.com`